IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA Plaintiff, v. EVGENIY MIKHAILOVICH BOGACHEV a/k/a "Slavik", a/k/a "Pollingsoon" Lermontova Str. 120-101 Anapa, Russian Federation "TEMP SPECIAL" "DED" "CHINGIZ 911" a/k/a/ "CHINGIZ" "MR. KYKYPYKY" Defendants.	)	Civil Action No. 14-0685 **FILED *EX PARTE*** **AND UNDER SEAL**

COMPLAINT

Plaintiff, the United States of America, by and through its undersigned counsel, alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521, and Federal Rule of Civil Procedure 65, to enjoin the Defendants from continuing to engage in wire fraud, bank fraud, and unauthorized interception of electronic communications in violation of Title 18, United States Code, Sections 1343, 1344, and 2511, by means of malicious computer software ("malware") known as Gameover Zeus ("GOZ") and "Cryptolocker."

2. GOZ is malware that steals banking and other online credentials from infected computers and enlists those computers into a "botnet" – a network of other infected computers controlled by the Defendants. Individual infected computers, or "bots," are controlled remotely

through a decentralized command and control ("C&C") system in which (a) ordinary infected computers, or "peers," remain in contact with each other; (b) specially selected peers called "proxy nodes" transmit commands and other information from the Defendants to the peers; and (c) a Domain Generation Algorithm ("DGA") is used to generate a large number of Internet domain names with which the infected computers communicate at least once a week.

3. Cryptolocker is a form of malware known as "ransomware," which infects computers, encrypts key files, and then demands a ransom of hundreds of dollars in order to return the encrypted files to a readable state. GOZ is one of the primary vehicles for infecting victim computers with Cryptolocker.

4. Together, GOZ and Cryptolocker have infected hundreds of thousands of computers around the world and have generated losses that exceed $100 million.

Parties

5. Plaintiff is the United States of America.

6. Defendant Evgeniy Mikhailovich Bogachev is citizen of Russia residing at Lermontova Str. 120-101, Anapa, Russian Federation. Bogachev is a leader of the criminal enterprise responsible for GOZ and Cryptolocker.

7. Defendants "Temp Special," "Ded," "Chingiz 911" a/k/a "Chingiz" and "mr. kykyprky" are individuals, believed to be located in either Russia or Ukraine, who assist in the administration of the GOZ botnet.

Jurisdiction and Venue

8. Subject matter jurisdiction lies pursuant to Title 18, United States Code, Sections 1345(a)(1) and 2521 and Title 28, United States Code, Sections 1331 and 1345.

9. Defendants are subject to the personal jurisdiction of this Court, having infected computers, used infected computers in furtherance of their scheme to defraud, initiated fraudulent money transfers, and engaged in unauthorized wiretapping, all within the Western District of Pennsylvania.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2).

The GOZ Scheme to Defraud and Unauthorized Interception

11. A botnet is a collection of compromised computers that are controlled, without the knowledge of the victims, by an unauthorized third party. A botnet can be used for many criminal purposes, including sending spam, stealing data, and committing financial fraud.

12. The GOZ botnet has been used for, among other purposes, the commission of fraudulent financial activity. The principal purpose of GOZ is to capture banking credentials from infected computers. One means by which GOZ accomplishes this is through "man-in-the-middle" attacks, in which GOZ intercepts sensitive information victims transmit from their computers.

13. To increase the effectiveness of such attacks, the Defendants use GOZ to inject additional code into victims' web browsers that changes the appearance of the websites victims are viewing. For example, if a GOZ-infected user were to visit a banking website that typically requests only a username and password, the defendants could seamlessly inject additional form fields into the website displayed in the user's web browser that also request the user's social security number, credit card numbers, and other sensitive information. Because these additional

fields appear to be part of the legitimate website users elected to visit, users are often defrauded into supplying the requested information, which is promptly intercepted by GOZ and transmitted to the defendants.

14. The Defendants use the intercepted credentials for fraudulent purposes, such as initiating or re-directing wire transfers from victims' accounts to accounts controlled by the GOZ organization overseas.

15. Victims of the GOZ scheme to defraud and unauthorized interception include, among others:

a. A composite materials company in the Western District of Pennsylvania, which lost more than $198,000 after an unauthorized wire transfer was initiated from its bank account using credentials stolen by the Defendants through the use of GOZ;

b. An Indian tribe in Washington which lost more than $277,000 after an unauthorized wire transfer was initiated from its bank account using credentials stolen by the Defendants through the use of GOZ;

c. A corporation operating assisted living facilities in Eastern Pennsylvania, which lost more than $190,800 after an unauthorized wire transfer was initiated from its bank account using credentials stolen by the Defendants through the use of GOZ;

d. A regional bank in Northern Florida, which lost nearly seven million dollars after an unauthorized wire transfer was initiated from its bank account using credentials stolen by the Defendants through the use of GOZ.

16. Since GOZ first emerged in September 2011, total losses attributable to GOZ exceed $100 million.

The Cryptolocker Scheme to Defraud

17. Cryptolocker is a malicious program designed to extract ransom payments from victims. After infecting a computer, Cryptolocker encrypts files on the infected computer's hard drive. Once the victim's files have been encrypted, Cryptolocker displays a notice on the victim's computer that demands payment of a ransom in exchange for the key that can decrypt the victim's files. The ransom varies in amount, but can reach up to $750 or more.

18. Victims who refuse to pay the ransom face significant data loss, since the encryption algorithm used by the defendants is effectively unbreakable.

19. Cryptolocker first emerged in mid-to-late 2013 and has infected more than 230,000 computers in the ensuing months, including more than 120,000 victims in the United States.

20. GOZ includes code that permits the defendants to install additional malicious software onto computers infected with GOZ. The defendants and their co-conspirators have used this capability to install Cryptolocker onto numerous computers within the GOZ botnet. Cryptolocker is thus a second prong of the GOZ scheme to defraud.

21. The Defendants also defraud victims of Cryptolocker by falsely informing them that (1) the private key needed to unlock their computers will be destroyed in 72 hours if they fail to pay the Cryptolocker ransom, and (2) that any attempt to remove Cryptolocker from the computer will result in the destruction of the private key.

22. The victims of Cryptolocker fraud scheme described above include:

a. An insurance company in Pittsburgh, Pennsylvania had critical business files encrypted by Cryptolocker. The company was able to repair the damage by using backup files, but was forced to send employees home while the repair work was completed. The company estimates its total loss at $70,000.

b. A restaurant operator in Florida had over 10,000 files encrypted by Cryptolocker, including the contents of the company's team training, franchise, and recipe folders. The company estimates that remediating the Cryptolocker infection has cost the company $30,000.

c. A local police department in Massachusetts had its main file server, including administrative documents, investigative materials, and digital photo mug shots, encrypted by Cryptolocker. To recover these critical files, the SPD was forced to pay the $750 ransom demanded by Cryptolocker.

d. A pest control company in North Carolina had its most critical files, including its customer database and schedule of appointments, as well as its backup server, encrypted by Cryptolocker. The company estimates that the Cryptolocker infection has cost the company approximately $80,000 to date.

COUNT I
(Injunctive Relief under 18 U.S.C. § 1345)

23. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

24. The Defendants are engaging in wire fraud, in violation of Title 18, United States Code, Section 1343, in that the defendants, having devised a scheme or artifice to defraud and for obtaining money by means of false or fraudulent pretenses, are transmitting and causing to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, and signals for the purpose of executing such scheme or artifice.

25. Pursuant to Title 18, United States Code, Section 1345(a) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the GOZ botnet and of computers infected with Cryptolocker.

COUNT II
(Injunctive Relief under 18 U.S.C. § 1345)

26. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

27. The Defendants are engaging in bank fraud, in violation of Title 18, United States Code, Section 1344, in that the Defendants are knowingly executing a scheme or artifice to defraud financial institutions insured by the Federal Deposit Insurance Corporation and to obtain moneys under the custody and control of these institutions by means of false and fraudulent pretenses and representations.

28. Pursuant to Title 18, United States Code, Section 1345(a) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the GOZ botnet.

COUNT III
(Injunctive Relief under 18 U.S.C. § 2521)

29. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

30. The Defendants are engaging in the unauthorized interception of electronic communications, in violation of Title 18, United States Code, Section 2511, in that the defendants are intentionally intercepting electronic communications, and are intentionally using and endeavoring to use the contents of electronic communications knowing that the information is obtained through the unauthorized interception of electronic communications.

31. Pursuant to Title 18, United States Code, Section 2521, the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the defendants and their agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the GOZ botnet.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that the Court:

A. Enter judgment in favor of the Government and against the Defendants;

B. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and and permanent injunction against the Defendants and their agents, servants, employees, and all persons and entities in active concert or participation with them from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity from engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

C. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and permanent injunction authorizing the Government to continue the malware disruption plan specified in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief for a period of six months, and requiring the entities specified in the Temporary Restraining Order to continue take the actions specified in the Temporary Restraining Order for a period of six months.

D. Order such other relief that the Court deems just and proper.

Dated: May 27, 2014

Respectfully submitted,

DAVID J. HICKTON

United States Attorney

By: /s/ Michael A. Comber
MICHAEL COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL

Assistant Attorney General

By: /s/ Ethan Arenson
ETHAN ARENSON
DAVID AARON
Trial Attorneys
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
DC Bar No. 473296 (Arenson)
NY Bar No. 3949955 (Aaron)
Ethan.Arenson@usdoj.gov
David.Aaron@usdoj.gov